

## UNITED STATES DISTRICT COURT

for the  
Western District of New York

In the Matter of the Search of )  
(Briefly describe the property to be searched )  
or identify the person by name and address) ) Case No. 18-mj-1186  
Location Data Concerning Mobile Telephone Facility )  
(305) 766-7154 )  
)

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the \_\_\_\_\_ District of \_\_\_\_\_ New Jersey \_\_\_\_\_ (identify the person or describe property to be searched and give its location): Location Data Concerning Mobile Telephone Facility (305) 766-7154, as more fully set forth in Attachment A which is attached hereto and incorporated by reference herein.

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized): Evidence pertaining to violations of Title 18, U.S.C. §§ 1029(a)(1), 1029(a)(4), and 1344, as more fully set forth in Attachment B which is attached hereto and incorporated by reference herein.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☐ contraband, fruits of crime, or other items illegally possessed;  
☐ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of \_\_\_\_\_ 18 \_\_\_\_\_ U.S.C. § \_\_\_\_\_ 1029(a) and 1344 \_\_\_\_\_, and the application is based on these facts: SEE AFFIDAVIT

☒ Continued on the attached sheet.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

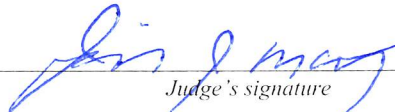
Michael L. Hamilton, Special Agent, U.S. Secret Service  
Printed name and title

Sworn to before me and signed in my presence.

Date:

10/23/18

City and state: Buffalo, New York



Judge's signature

JEREMIAH J. MCCARTHY, U.S. Magistrate Judge  
Printed name and title

**AFFIDAVIT IN SUPPORT OF SEARCH WARRANT**

I, Michael L. Hamilton, being duly sworn, depose and state:

1. I have been employed as a Special Agent with the United States Secret Service (USSS) since 2017. The USSS is an agency within the Department of Homeland Security (DHS), which is a department within the executive branch of the United States Government. I have received formal training in the investigation of crimes involving Bank Fraud and Access Device Fraud. I have also received training from the Federal Law Enforcement Training Center, Glynco Georgia and the United States Secret Service, Beltsville, Maryland. Prior to my employment with USSS, I served for over seven years in the Department of Defense as an Army Officer, where I worked multiple intelligence-based investigations involving crimes against national security.

2. I make this affidavit in support of an application for a search warrant for information associated with a certain cellular telephone assigned call number (305) 766-7154 ("the SUBJECT PHONE") that is stored at premises controlled by T-Mobile, a wireless telephone service provider headquartered at 4 Sylvan Way, Parsippany, NJ 07054. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. § 2703(c)(1)(A) to require T-Mobile to disclose to the government copies of the information further described in Section I of Attachment B. Upon receipt of the information described in

Section I of Attachment B, government-authorized persons will review the information to locate items described in Section II of Attachment B.

3. The statements made in this affidavit are based upon my involvement in this investigation, as well as information provided to me by other law enforcement officers involved in this investigation, and upon my training and experience. Because this affidavit is being submitted for the limited purpose of seeking a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of violations of Title 18, United States Code, Sections 1029(a)(1) (production, use, or trafficking in one or more counterfeit access devices); 1029(a)(4) (production, trafficking, or possession of device-making equipment); and 1344 (bank fraud) exists on the property listed in Attachment A.

#### **I. STATUTORY DEFINITIONS**

4. Pursuant to Title 18, United States Code, Section 1029(e)(1), the term “access device” means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument).

5. Pursuant to Title 18, United States Code, Section 1029(e)(2), the term “counterfeit access device” means any access device that is counterfeit, fictitious, altered, or forged, or an identifiable component of an access device or a counterfeit access device.

6. Pursuant to Title 18, United States Code, Section 1029(e)(6), the term “device-making equipment” means any equipment, mechanism, or impression designed or primarily used for making an access device or a counterfeit access device.

## **II. THE INVESTIGATION AND FACTUAL BASIS**

7. On or about October 10, 2018, at approximately 8:03 p.m., JORGE ALBERTO-ALVAREZ (“ALVAREZ”) attempted to enter the United States at the Peace Bridge Port of Entry, located in Buffalo, NY. During a primary inspection by Customs and Border Patrol (CBP) Officer Kanfesor, ALVAREZ stated that he had visited family in Detroit, Michigan, and that he was planning to drive back to Chicago, Illinois so that he could fly back to Miami, Florida. Based on inconsistencies in ALVAREZ’s stated travel itinerary, Officer Kandefer initiated a trunk inspection. During the inspection, Officer Kandefer observed a suitcase, and in the suitcase was a small box containing a large quantity of various credit, debit, and bank cards bearing names other than ALVAREZ. As a result, ALVAREZ was sent for a secondary inspection and a further search of his vehicle.

8. During secondary inspection, CBP Officer Tabone asked ALVAREZ about his purpose for travel. ALVAREZ stated that he was on a mini vacation, that he traveled by air

from Miami to Chicago, and then rented a car and drove to Michigan to attempt to meet up with a woman he had been communicating with on Facebook.

9. During the search of ALVAREZ's vehicle, Officer Tabone searched a black backpack in the backseat of the vehicle and discovered various gas station security seals, a Bluetooth magnetic card reader, a Lenovo Yoga Laptop Computer, and a Samsung Galaxy S9+ cellular telephone. During a search of the suitcase in the trunk of the vehicle, CBP Officer LaRosa located sixteen skimming devices, which are electronic communication devices consistent with those used in ATM skimming schemes. Additionally found was a small tool kit containing a battery-operated drill, various drill bits, Allen wrench sets, and pry bars. Inside the small box in the suitcase was discovered a total of 90 credit and debit cards. Using a credit card reader, CBP determined that all of the cards appeared to have various names and account information encoded on them, and on the reverse side of the card, a four digit number was written in black marker. A subsequent patdown of ALVAREZ revealed 11 bankcards in his wallet, with 2 of the cards having various names and account information encoded on them. Additionally located in ALVAREZ's wallet was a New Jersey driver's license in the name of another individual but containing the photograph of ALVAREZ. Your affiant has determined that this New Jersey driver's license is counterfeit.

10. At approximately 1:02 a.m. on October 11, 2018, Special Agent Colafranceschi with Homeland Security Investigations (HSI) interviewed ALVAREZ in the presence of CBP officers. During the interview, ALVAREZ stated that he attempted to meet up with a friend in Michigan, but after being unable to find her, he decided to enter Canada to visit Niagara

Falls, Ontario. When questioned about the items located in his vehicle, ALVAREZ stated he found the items next to a garbage pile in Miami, Florida. ALVAREZ admitted that he knew the cards were fraudulent and that he tried to use 3 of them at a gas station but was declined. ALVAREZ stated he used one of the names on the fraudulent cards to obtain a fraudulent New Jersey driver's license via the internet. ALVAREZ claimed that his friend in Michigan was going to buy all of the items that were found in his car for \$4,000, and that was the reason for his travel.

11. At approximately 3:30 a.m., your affiant was contacted by HSI and was requested to respond to the Peace Bridge. Upon arrival, HSI informed your affiant that CBP had conducted a preliminary border search of ALVAREZ's Samsung Galaxy S9+ cellular telephone, discovering multiple text messages from an unknown individual. These text messages contained addresses and photographs of multiple gas stations, including a gas station that appeared to be in the State of Tennessee. Moreover, HSI informed me that one of the photographs contained on ALVAREZ's Samsung phone was a photograph of gas station security seals, and that according to CBP, the photo appeared to be from approximately 1 year ago. At that time, I inspected the items seized from ALVAREZ's vehicle. In particular, one of the items was a card reader/encoder, which is a device used, along with a computer, to load electronic data onto the magnetic stripe of a card. In addition, I observed 16 internal skimming devices ("skimmers"), and a customized cable, which appears to have been used to connect the computer to the skimming devices. In reviewing all of the credit and debit cards seized, a total of 93 cards were found to be counterfeit, meaning that the account details on the magnetic stripe of the card do not match the embossed

information on the card. The account numbers contained on the cards meet the definition of access devices since those account numbers can be used to obtain money, and the re-encoded cards that contain account information meet the definition of counterfeit access devices because they were not issued by the appropriate bank or credit card company. The computer, card encoder, cables and skimmers are device-making equipment since they are all used to create counterfeit access devices. The skimmers are used to collect the account numbers. The cables are used to retrieve the information from the skimmers to the computer. The computer and the card encoder is used to alter the card's magnetic stripe to become a counterfeit access device.

12. In addition to the counterfeit access devices and manufacturing materials, ALVAREZ possessed 65 gas station security seals, some of which contained Chevron and Sunoco gas station logos. Similar skimming schemes utilize telephonic reconnaissance, similar to the gas station photographs observed on ALVAREZ's phone, to target specific gas station pumps. In order to install an internal skimming device, an individual must destroy the existing security seal to gain access to the gas pump. After the internal skimming device is installed, the individual will replace the destroyed security seal with a counterfeit one, similar to those found in ALVAREZ's possession.

13. In similar skimming schemes, the computer serves as the data storage center for compromised credit and debit card information, as well as the conduit for said information to be transferred onto counterfeit access devices. The computer is often transported directly to the skimming site, so that the compromised data can be quickly uploaded. At the time of

his arrest, ALVAREZ possessed a “Cyber Power” 12 volt car charger with a 120V (three prong) output. ALVAREZ’s Lenovo Yoga Laptop Computer was the only electronic device found in the vehicle that was compatible with the “Cyber Power” charger, indicating the computer was being used/powered inside the vehicle.

14. Based on my training and experience, I am familiar with fraudulent schemes to obtain money using a skimming device. A skimming device is essentially an electronic device that captures information contained on a credit or debit card, and can be attached on the face plate of where a card is swiped, or can be placed internally at point of sale terminals more discreetly capture the payment card data. In particular, I am aware of recent fraudulent activity at gas stations, where internal skimming devices are installed to capture the payment card data for cards used purchase gasoline. The information from the skimming device is usually retrieved physically or remotely using Bluetooth or WiFi. At that point, the downloaded information can then be transferred onto blank cards, creating “clones” of the original bankcards.

15. Following the arrest of ALVAREZ, investigation revealed that ALVAREZ booked an airline reservation with Delta Airlines for travel on August 28, 2018, from Los Angeles, CA, to Seattle, WA, and to Anchorage, AK. Additionally, ALVAREZ booked an airline reservation with American Airlines for travel on September 24, 2018, from Denver, CO, to Dallas, TX, and to Memphis, TN. However, during the HSI interview of ALVAREZ on October 11, 2018, ALVAREZ stated that he was self-employed as an air conditioning repair technician, and that he mainly services the Miami, FL area and surrounding suburbs.



ALVAREZ also indicated prior travel to Las Vegas, NV, Denver, CO, and Orlando, FL, but did not mention any travel to Washington, Alaska, Texas, and/or Tennessee.

### **III. REQUESTED INFORMATION**

16. In my training and experience, I have learned that T-Mobile is a company that provides cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of the cellular telephones to which they provide service, including cell-site data, also known as “tower/face information” or “cell tower/sector records.” Cell-site data identifies the “cell towers” (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the “sector” (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate location of the cellular telephone but is typically less precise than other types of location information, such as E-911 Phase II data or Global Positioning Device (“GPS”) data.

17. Based on my training and experience, I know that T-Mobile can collect cell-site data about the SUBJECT PHONE. I also know that wireless providers such as T-Mobile typically collect and retain cell-site data pertaining to cellular phones to which they provide service in their normal course of business in order to use this information for various business-related purposes.

18. Based on my training and experience, I know that wireless providers such as T-Mobile typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless telephone service. I also know that wireless providers such as T-Mobile typically collect and retain information about their subscribers' use of the wireless service, such as records about calls or other communications sent or received by a particular phone and other transactional records, in their normal course of business. In my training and experience, this information may constitute evidence of the crimes under investigation because the information may assist in the identification of where ALVAREZ travelled and where skimming devices may have been installed on gas station pumps. The location information, including cell-site data, can be cross-checked against other travel related information already obtained in the case, which can help determine whether ALVAREZ installed and/or used skimming devices at particular gas stations.

#### **IV. AUTHORIZATION REQUEST**

19. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

20. I further request that the Court direct T-Mobile to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrant will be served on T-Mobile, who will then compile the

requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

21. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed for 60 days, subject to further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation, including by giving targets an opportunity to destroy or tamper with evidence, change patterns of behavior, notify confederates, and flee from prosecution.



Michael L. Hamilton, Special Agent  
United States Secret Service

Sworn and subscribed to before me  
this 23<sup>rd</sup> day of October 2018.



HON. JEREMIAH J. MCCARTHY  
United States Magistrate Judge

**ATTACHMENT A**  
**Property to be Searched**

This warrant applies to records and information associated with the cellular telephone assigned call number (305) 766-7154 (“the Account”) that are stored at premises controlled by T-Mobile (“the Provider”), located at 4 Sylvan Way, Parsippany, NJ 07054.

**ATTACHMENT B**  
**The Items to be Searched for and Seized**

**I. Information to be Disclosed by the Provider**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A for the time period October 1, 2017, to the present:

1. The following information about the customers or subscribers of the Account:

- a. Names (including subscriber names, user names, and screen names);
- b. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
- c. Local and long distance telephone connection records;
- d. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;
- e. Length of service (including start date) and types of service utilized;
- f. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");
- g. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and
- h. Means and source of payment for such service (including any credit card or bank account number) and billing records.

2. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Account, including:
  - a. the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and
  - b. information regarding the cell towers and sectors through which the communications were sent and received.

## **II. Information to be Searched for and Seized by the Government**

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. § 1029(a)(1), 1029(a)(4), and 1344 by any user of the Account during the period October 1, 2017, to the present.